Serdica

Mathematical Journal

Сердика

Математическо списание

For further information on
Serdica Mathematical Journal
which is the new series of
Serdica Bulgaricae Mathematicae Publicationes
visit the website of the journal http://www.math.bas.bg/~serdica
or contact: Editorial Office
Serdica Mathematical Journal
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: serdica@math.bas.bg

Serdica Math. J. **30** (2004), 303–324

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

MINIMAL CODEWORDS IN LINEAR CODES

Yuri Borissov, Nickolai Manev

Communicated by V. Brînzănescu

Abstract. Cyclic binary codes $\mathcal{C}$ of block length $n = 2^m - 1$ and generator polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, $(s, m) = 1$, are considered. The cardinalities of the sets of minimal codewords of weights 10 and 11 in codes $\mathcal{C}$ and of weight 12 in their extended codes $\widehat{\mathcal{C}}$ are determined.

The weight distributions of minimal codewords in the binary Reed-Muller codes $RM(3, 6)$ and $RM(3, 7)$ are determined. The applied method enables codes with larger parameters to be attacked.

1. Introduction. Let $\mathcal{C}$ be a linear code over the field of q elements $\mathbb{F} = GF(q)$, i.e. a subspace of the n-dimensional vector space $\mathbb{F}^n$. As usual, the parameters n, k and d denote length, dimension and minimum distance, respectively, and we will refer a code $\mathcal{C}$ with these parameters as an $[n, k, d]$ code. We also use the notation $[n] := \{1, 2, \ldots, n\}$ for the set of code coordinates. A *support* of a vector $\mathbf{c}$ is defined as $\mathrm{supp}(\mathbf{c}) = \{i \in [n] : c_i \neq 0\}$. If $\mathrm{supp}(\mathbf{c}') \subset \mathrm{supp}(\mathbf{c})$ (respectively, $\subseteq$), we also write $\mathbf{c}' \prec \mathbf{c}$ (respectively, $\preceq$).

2000 *Mathematics Subject Classification:* 94B05, 94B15.
Key words: minimal codewords; cyclic codes; binary Reed-Muller code.

Definition. *Let $\mathcal{C}$ be a $q-$ary linear code. A nonzero codeword $\mathbf{c} \in \mathcal{C}$ is called* **minimal** *if its support does not contain the support of any other nonzero codeword as a proper subset.*

For the first time the sets of minimal codewords in linear codes were considered in connection with a decoding algorithm (Tai-Yang Hwang [11]). A more detailed description of the role of minimal codewords in the so called "gradient-like decoding algorithm" can be found in [2] and [3, Ch. 7]. Additional interest to minimal codewords was sparked by the work of J. Massey [17], where it was shown that they describe minimal access structures in secret-sharing schemes based on linear codes. For definitions of a secret-sharing scheme and access structure determined by a linear code we refer the reader to [18]. Minimal codewords were also addressed in [1] for the Euclidean space.

It seems to be quite difficult to describe the set of minimal codewords for an arbitrary linear code even in the binary case. The problem has been completely solved only for q-ary Hamming code and for the second order binary Reed-Muller code $RM(2, m)$ [2]. In the same paper [2] Ashikhmin and Barg also determine the average number of minimal codewords of the ensemble over a random linear code and analyze the asymptotic behavior of the structure of minimal codewords in long codes. For the general case of the r^{th} order binary Reed-Muller codes and for the other types of codes only partial results have been obtained till now.

In the binary case the weights of interest are values w:

$$2d \leq w \leq n - k + 1,$$

since for them both minimal and non-minimal codewords can exist according to (iii) and (iv) of Proposition given in the next section.

In [7] Borissov, Manev and Nikova obtain the number of non-minimal codewords of weight $2d_{\min}$ and some other results about minimal/non-minimal codewords in the r^{th} order binary Reed-Muller code $RM(r, m)$. BCH codes are discussed in [6].

In this paper we present some results about minimal codewords in a class of cyclic codes and in third order binary Reed-Muller codes $R(3, m)$. What consolidates these two cases is the algebraic approach to studying them.

The paper is organized as follows: in the next section we give the necessary definitions and results which we will use.

In Section 3 we determine the cardinalities of the sets of minimal (non-minimal) codewords of weights 10 and 11 in the considered cyclic code $\mathcal{C}$ as well as of weight 12 in its extended code $\widehat{\mathcal{C}}$. The interest in weights 10 and 12 is due

to the fact that they are the first weights of $\mathcal{C}$ and $\widehat{\mathcal{C}}$, respectively, for which both minimal and non-minimal codewords exist.

In Section 4 we study minimal codewords in binary Reed-Muller codes but we apply an algebraic approach to the problem in contrast to the geometrical one used in [7]. We explore the classical algebraic idea: instead of direct studying of an algebraic structure, studying its sub- and quotient structures.

2. Some general remarks and necessary results. Herein we only recall the definitions of the codes which are studied in the next two sections and refer the reader to [16] for details.

The code $\mathcal{C}$ over the finite field with q elements $\mathbb{F} = GF(q)$ is called *cyclic* if any cyclic shift of a codeword is also a codeword, i.e. whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then also $(c_1, \ldots, c_{n-1}, c_0) \in \mathcal{C}$. By mapping

$$\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \longrightarrow c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

we identify any cyclic code $\mathcal{C}$ with an ideal of the algebra $\mathcal{F}_n = \mathbb{F}[x]/(x^n - 1)$ of polynomials over $\mathbb{F}$ modulo $x^n - 1$. The polynomial $g(x)$ generating the ideal corresponding to $\mathcal{C}$ is referred as a *generator polynomial* of $\mathcal{C}$. Let α be a primitive element of the field $GF(q^m)$. As usual we denote the minimal polynomial of α^k over $\mathbb{F}$ by $m_k(x)$. The powers of α which are zeros of $g(x)$ are called *zeros* of the cyclic code $\mathcal{C}$ and the generator polynomial $g(x)$ is a product of their minimal polynomials over $\mathbb{F}$.

Let $\mathcal{P}_m$ be the set of Boolean polynomials of m variables $x_1, \ldots, x_m$ and $f \in \mathcal{P}_m$. The binary vector $\mathbf{f} = (f(0, \ldots, 0), \ldots, f(1, \ldots, 1))$ of length 2^m is referred to be the binary vector associated with (or corresponding to) the Boolean polynomial $f(\mathbf{x})$.

For any m and r, $0 \leq r \leq m$, *the binary* r^{th} *order Reed-Muller code* $RM(r, m)$ is defined as the set of all binary codewords $\mathbf{f}$ of length $n = 2^m$ associated with Boolean polynomials $f(x_1, x_2, \ldots, x_m)$ of degree at most r.

$RM(r, m)$ has block length $n = 2^m$, dimension $k = 1 + \binom{m}{1} + \cdots + \binom{m}{r}$, and minimum distance $d = 2^{m-r}$. The full automorphism group of $RM(r, m)$ for $r \leq m - 2$ is the general affine group $GA(m, 2)$.

Also the codewords of minimum weight in $RM(r, m)$ are precisely the incidence vectors of the $(m-r)$-dimensional affine subspaces (called also $(m-r)$-flats) of the affine geometry $AG(m, 2)$ and they span $RM(r, m)$. Therefore, one can use both algebraic and geometric language to study Reed–Muller codes, and each of them has its advantages.

Now, let return to the main goal of our study - minimal codewords. Their basic properties are listed in Proposition. Some of them are direct consequence from the definitions but the proof of all properties can be found in [2].

Proposition ([2]). *Let $\mathcal{C}$ be a q-nary $[n,k,d]$ linear code.*

(i) $\mathbf{c} \in \mathcal{C}$ *is minimal if and only if* **(iff)** $\mathbf{c} \succeq \mathbf{c}'$, $0 \neq \mathbf{c}' \in \mathcal{C}$, *implies* $\mathbf{c}' = \alpha\mathbf{c}$ *for a nonzero element* $\alpha \in \mathbb{F}^*$.

(ii) *Let* $\mathbf{H}$ *be a parity check matrix of* $\mathcal{C}$. *The subset* $S \subset [n]$ *is a support of a minimal codeword if and only if* $\mathrm{rank}(\mathbf{H}(S)) = |S| - 1$, *where* $\mathbf{H}(S)$ *is the matrix formed by the columns of* $\mathbf{H}$ *indexed by* S.

(iii) *If* $\mathbf{c}$ *is a minimal codeword in* $\mathcal{C}$, *then* $wt(\mathbf{c}) \leq n - k + 1$

(iv) *Every support of size* $\leq d\left(1 + \dfrac{1}{q-1}\right)$ *is minimal with respect to* $\mathcal{C}$.

(v) *Any codeword* $\mathbf{c} \in \mathcal{C}$ *is linear combination of all minimal codewords that it covers (in sense of inclusion of supports).*

(vi) *Multiplication of a codeword by an element of* $\mathbb{F}$ *and permutation of its coordinate positions are transformations which preserve the property of the codeword to be minimal.*

(vii) *Let* $\mathcal{C}$ *be a binary code. If* $\mathbf{c}$ *is a non-minimal codeword in* $\mathcal{C}$, *there is a pair of nonzero codewords* $\mathbf{c}_1 \prec \mathbf{c}$ *and* $\mathbf{c}_2 \prec \mathbf{c}$ *with disjoint supports, such that* $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2$.

We end this section with the following lemma. We include it here since it concerns basic properties of minimal codewords in binary linear codes, nevertheless we shall use it in Section 3.

Recall that the *extended code* of a q-ary $[n,k,d]$ code $\mathcal{C}$ is called the $[n+1,k,d_1]$ code

$$\widehat{\mathcal{C}} = \{\widehat{\mathbf{c}} = (c_1,\ldots,c_n|c_\infty) \mid (c_1,\ldots,c_n) \in \mathcal{C},\ c_\infty = c_1 + \cdots + c_n\}.$$

In the binary case the minimum distance $d_1 = d+1$, if d is odd, and $d_1 = d$, if d is even. It is said also that $\widehat{\mathcal{C}}$ is obtained *by adding general parity check.*

Lemma 1. *Let* $\mathcal{C}$ *be a binary linear code of length* n, $\mathcal{C}^0$ *be its subcode of codewords of even weight and* $\widehat{\mathcal{C}}$ *be its extended code. Denote* M_w, M_w^0 *and* $\widehat{M_w}$

the number of minimal codewords of weight w in codes $\mathcal{C}$, $\mathcal{C}^0$ and $\widehat{\mathcal{C}}$, respectively. Then

$$\widehat{M}_{2j} = M_{2j-1} + M^0_{2j}.$$

If $\widehat{\mathcal{C}}$ has a transitive group of automorphisms then

$$M_{2j-1} = \frac{2j}{n+1}\widehat{M}_{2j}; \qquad M^0_{2j} = \left(1 - \frac{2j}{n+1}\right)\widehat{M}_{2j}.$$

P r o o f. If $c \in \mathcal{C}$ is of weight $2j-1$ then $\widehat{c} = (c|c_\infty),\ c \in \mathcal{C},\ c_\infty = 1$ is a minimal codeword of weight $2j$ in $\widehat{\mathcal{C}}$ **iff** c is minimal in $\mathcal{C}$. When $c \in \mathcal{C}$ with $wt(c) = 2j$ is minimal, $\widehat{c} = (c|0)$ is a minimal codeword in $\widehat{\mathcal{C}}$, too. But it is possible that $\widehat{c} = (c|0)$ of weight $2j$ to be minimal codeword of $\widehat{\mathcal{C}}$ (i.e. c to be minimal in $\mathcal{C}^0$) while c is a non-minimal codeword of $\mathcal{C}$ – when it covers codewords of $\mathcal{C}$ of odd weight. Therefore $M^0_{2j} \geq M_{2j}$ and

$$\widehat{M}_{2j} = M_{2j-1} + M^0_{2j}.$$

In the case when the automorphism group of $\widehat{\mathcal{C}}$ is transitive we can proceed as in Theorem 14 of [16, Ch.8] to obtain the statement of the lemma. □

3. Cyclic codes of block length $n = 2^m - 1$ and a generator polynomial $g(x) = m_1(x)m_{2^s+1}(x)$. Consider cyclic binary codes of block length $n = 2^m - 1$ with a generator polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, i.e. cyclic codes with zeros α and α^{2^s+1}, where α is a primitive element of the field $GF(2^m)$. As usual a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ is identified by the polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ when $\mathbf{c} \in \mathcal{C}$ **iff** $c(\alpha) = c(\alpha^{2^s+1}) = 0$. For $(s, m) = 1$ these codes are quasi-perfect codes with minimum distance 5 [9]. It is interesting that the considered class of codes contains the primitive BCH codes (the case $s = 1$) and all its codes have the same weight enumerator [16, Ch. 15]. But the codes with $s \neq 1$ are not isomorphic to the BCH codes [4].

Our goal is to determine the cardinalities of the sets of minimal (non-minimal) codewords of weights 10 and 11 in $\mathcal{C}$ as well as such codewords of weight 12 in its extended code $\widehat{\mathcal{C}}$.

As usual $\mathrm{Tr}_\delta : GF(2^m) \to GF(2^\delta),\ \ \delta|m$, denotes the trace function defined by

$$\mathrm{Tr}_\delta(x) = x + x^{2^\delta} + x^{2^{2\delta}} + \cdots + x^{2^{m-\delta}}.$$

Also, we will write only $\mathrm{Tr}(x)$ instead of $\mathrm{Tr}_1(x)$.

To prove our results we need the following lemmas. The first one is Lemma 2 which is a consequence of Welch's theorem cited in [5, 16.46] for $a = 1$. It is also a partial case ($e = 1$) of Theorem 11.11 in [15].

Lemma 2 ([5],[15]). *The number of nonzero cubes $\gamma = x^3$ in the field $GF(2^{2l})$ with zero trace $\mathrm{Tr}(\gamma) = 0$ equals*

$$p = \frac{1}{3}\left(2^{2l-1} - (-1)^l.2^l - 1\right).$$

Lemma 3. *If $(s, m) = \delta$ the equation*

$$z^{2^s} + z + \gamma = 0$$

has

– *exactly 2^δ roots in $GF(2^m)$, when $\mathrm{Tr}_\delta(\gamma) = 0$;*
– *no solutions in $GF(2^m)$, when $\mathrm{Tr}_\delta(\gamma) \neq 0$.*

P r o o f. Suppose that $\theta \in GF(2^m)$ is a solution of the equation. Then the equality $\mathrm{Tr}_\delta(\theta^{2^s}) = \mathrm{Tr}_\delta(\theta)$ yields $\mathrm{Tr}_\delta(\gamma) = 0$. Therefore, the equation has no roots in $GF(2^m)$ when $\mathrm{Tr}_\delta(\gamma) \neq 0$.

Now let $\mathrm{Tr}_\delta(\gamma) = 0$ and let us consider the linear map over $GF(2)$

$$\varphi : \left| \begin{array}{c} GF(2^m) \longrightarrow GF(2^m) \\ z \longrightarrow z^{2^s} + z \end{array} \right.$$

Then

$$\ker\varphi = \{z \in GF(2^m) \mid z^{2^s} + z = 0\} = GF(2^m) \cap GF(2^s) = GF(2^\delta)$$

and

$$A = \{\gamma \in GF(2^m) \mid \mathrm{Tr}_\delta(\gamma) = 0\} \supseteq \mathrm{Im}\varphi$$

since $\mathrm{Tr}_\delta(z^{2^s} + z) = 0$. But

$$|A| = \frac{|GF(2^m)|}{|GF(2^\delta)|} = 2^{m-\delta}$$

and $\dim \mathrm{Im}\varphi = m - \dim\ker\varphi = m - \delta$, i.e. $|\mathrm{Im}\varphi| = 2^{m-\delta}$

Hence

$$\mathrm{Im}\varphi = \{\gamma \in GF(2^m) | \, \mathrm{Tr}_\delta(\gamma) = 0\}$$

Therefore, for any $\gamma \in GF(2^m)$ with $\mathrm{Tr}_\delta(\gamma) = 0$ there exist $|\ker \varphi| = 2^\delta$ values z such that $z^{2^s} + z = \gamma$. $\square$

Remark. The equation $z^{2^s} + z + \gamma = 0$ was first considered by Dumer [10] in order to prove that the class of codes treated in the next lemma are uniformly packed. He proved that in the case $(m, s) = 1$ the equation has a solution in $GF(2^m)$ **iff** $\mathrm{Tr}(\gamma) = 0$.

Lemma 4. *Let $\mathcal{C}$ be a binary cyclic code of length $n = 2^m - 1$ and a generator polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, where $(s, m) = 1$.*

If m is odd then for any pair $\{i, j\}$, $0 \le i < j \le n - 1$, the number of codewords of weight 5 with nonzero positions i and j is

$$\lambda = \frac{n-7}{6}.$$

If $m = 2l$ then this number
– for np pairs $\{i, j\}$ is equal to

$$\lambda = p - 1 = \frac{1}{3}[2^{2l-1} - (-1)^l 2^l - 4],$$

– for the remaining $2nq = n(2^{m-1} - 1 - p)$ pairs $\{i, j\}$ is equal to

$$\mu = q - 1 = \frac{1}{3}[2^{2l-1} + (-1)^l 2^{l-1} - 4],$$

where p is determined in Lemma 2 and $q = (2^{m-1} - 1 - p)/2$.

Remark. The values of λ and μ are the same as for the BCH codes (case $s = 1$) nevertheless the proof of the lemma is slightly more complicated.

P r o o f. Since $\mathcal{C}$ is a cyclic code, without loss of generality (w.l.o.g.) we may assume that $i = 0$, i.e. we may consider only pairs $\{0, j\}$, $0 < j \le n - 1$.

Let $c(x) \in \mathcal{C}$ be a codeword of weight 5 (recall that $\mathcal{C}$ is an $[n,\ n-2m,\ 5]$ code), i.e.

$$c(x) = 1 + x^j + x^{i_1} + x^{i_2} + x^{i_3}, \ \ 0 < i_1 < i_2 < i_3 \le n - 1, \ j \ne i_1, i_2, i_3.$$

The equalities $c(\alpha) = c(\alpha^{2^s+1}) = 0$ imply

$$(1) \qquad \left| \begin{array}{ll} y_1 + y_2 + y_3 & = 1 + \beta \\ y_1^{2^s+1} + y_2^{2^s+1} + y_3^{2^s+1} & = 1 + \beta^{2^s+1}, \end{array} \right.$$

where $y_1 = \alpha^{i_1}$, $y_2 = \alpha^{i_2}$, $y_3 = \alpha^{i_3}$, $\beta = \alpha^j \neq 0, 1$. Obviously y_1, y_2, y_3 should be different and $y_\nu \in GF(2^m)$, $y_\nu \neq 0, 1, \beta$.

Replacing $y_\nu = x_\nu + (1 + \beta)$ $\nu = 1, 2, 3,$ we get

$$\left| \begin{array}{ll} x_1 + x_2 + x_3 & = 0 \\ x_1^{2^s+1} + x_2^{2^s+1} + x_3^{2^s+1} & = \beta + \beta^{2^s}, \end{array} \right. \tag{2}$$

where $x_\nu \neq 0, 1, \beta$ and all x_ν are different.

The number λ of codewords of weight 5 with nonzero coordinates $\{0, j\}$ coincides with the number of unordered triples $\{x_1, x_2, x_3\}$ of pairwise different elements $x_\nu \in GF(2^m)$ satisfying (2) and the additional conditions $x_\nu \neq 0, 1, \beta, \beta{+}1$.

Replacing $x_1 = x_2 + x_3$ from the first equation into the second one we get

$$\beta + \beta^{2^s} = \sum x_\nu^{2^s+1} = (x_2 + x_3)^{2^s}(x_2 + x_3) + x_2^{2^s+1} + x_3^{2s+1} = x_2^{2^s} x_3 + x_2 x_3^{2^s},$$

which after dividing by $x_3^{2^s+1} \neq 0$ gives

$$\left(\frac{x_2}{x_3}\right)^{2^s} + \frac{x_2}{x_3} + \frac{\beta + \beta^{2^s}}{x_3^{2^s+1}} = 0.$$

Therefore

$$x_1 = (1 + z)t, \quad x_2 = zt, \quad x_3 = t,$$

where $t \in GF(2^m)^* = GF(2^m) \setminus \{0\}$, $t \neq 1, \beta, \beta + 1$ and $z = z(t) \in GF(2^m)$, $z \neq 0, 1$, is a solution of

$$z^{2^s} + z + \frac{\beta^{2^s} + \beta}{t^{2^s+1}} = 0. \tag{3}$$

Conversely, any triple $\{(1 + z)t, zt, t\}$ where z is a solution of (3), $z \in GF(2^m)$ and $t \in GF(2^m)^*$, $t \neq 1$, β, $\beta + 1$ satisfies the system (2). In addition, since $\beta \neq 0, 1$ then $z \neq 0, 1$ which with $t \neq 0$ implies x_ν pairwise different.

Due to the symmetry with respect to x_1, x_2, x_3 any triple $\{x_1, x_2, x_3\}$ will be obtained three times – for three values of t: t, zt, $(1 + z)t$. Besides, for $t = 1$ we have $(z + \beta)^{2^s} = z + \beta$, i.e. $z_1 = \beta$, $z_2 = 1 + \beta$ which gives the triple $\{1 + \beta, \beta, 1\}$. Similarly

$$t = \beta \;\Rightarrow\; z_1 = \beta^{-1}, z_2 = 1 + \beta^{-1} \;\Rightarrow\; \{\beta + 1, 1, \beta\};$$

$$t = 1 + \beta \;\Rightarrow\; z_1 = (1 + \beta)^{-1}, z_2 = \beta/(1 + \beta) \;\Rightarrow\; \{1, \beta, 1 + \beta\}.$$

Thus all inadmissible values of t give one and the same triple $\{1, \beta, 1 + \beta\}$.

Therefore, the number of codewords of weight 5 with nonzero coordinates $\{0, j\}$ for given $j \neq 0$ (i.e. for given $\beta \neq 0, 1$) is equal to

$$\frac{1}{3}R_\beta - 1,$$

where R_β is the number of triples $((1+z)t, zt, t)$, $t \in GF(2^m)^*$, i.e. the number of $t \in GF(2^m)^*$ for which (3) has a solution in $GF(2^m)$. But according to Lemma 3, (3) has roots (exactly 2) in $GF(2^m)$ **iff**

$$\text{Tr}\left(\frac{\beta^{2^s}+\beta}{t^{2^s+1}}\right) = 0. \tag{4}$$

Hence R_β coincides with the number of t for which (4) holds.

Now, let m be odd. We have to prove that R_β does not depend on β and calculate it.

It is easy to see that for $(s, m) = 1$,

$$(2^s+1, 2^m-1) = \begin{cases} 1, & m \text{ – odd} \\ 3, & m \text{ – even.} \end{cases}$$

Thus, in the case of m being odd, t^{2^s+1} runs through all nonzero elements of $GF(2^m)$ when t runs through $GF(2^m)^*$. Hence for any fixed $\beta \neq 0, 1$ $(\beta^{2^s} + \beta)/t^{2^s+1}$ runs through all elements of $GF(2^m)^*$. ($\beta^{2^s}+\beta \neq 0$, for $\beta \in GF(2^m)$, $\beta \neq 0, 1$)

Therefore exactly $2^m/2 - 1 = 2^{m-1} - 1$ of $(\beta^{2^s} + \beta)/t^{2^s+1}$ will be with a zero trace, i.e. $R_\beta = 2^{m-1} - 1 = (n-1)/2$. Hence the number λ of codewords of weight 5 with nonzero coordinates $\{0, j\}$ is equal to

$$\lambda = \frac{1}{3}\frac{n-1}{2} - 1 = \frac{n-7}{6}.$$

In the case of $m = 2l$, $(2^s + 1, 2^m - 1) = 3$. Thus $t^{2^s+1} = u^3$ and will take only $(2^m - 1)/3$ values (the cubes) when t runs through $GF(2^m)^*$. Then $(\beta^{2^s} + \beta)/t^{2^s+1}$ has the same form α^{3k}, α^{3k+1}, or α^{3k+2} as $\beta^{2^s} + \beta$, thus, $(\beta^{2^s} + \beta)/t^{2^s+1}$ takes any value α^{3k}, respectively α^{3k+1} or α^{3k+2}, when t runs through $GF(2^m)^*$. In addition, since $(\alpha^{3k+1})^2 = \alpha^{3r+2}$ and vice versa, and $\text{Tr}(\gamma) = \text{Tr}(\gamma^2)$, the number of elements of the form α^{3k+1} with zero trace equals the number of elements of the form α^{3k+2} with zero trace, too. According to Lemma 2 the number of cubes with zero trace is

$$p = \frac{1}{3}\left(2^{2l-1} - (-1)^l.2^l - 1\right).$$

Hence the number of elements of the type $\gamma = \alpha^{3k+1}$ with $\mathrm{Tr}(\gamma) = 0$, respectively one of the form α^{3k+2}, is

$$q = \frac{2^{m-1} - 1 - p}{2} = \frac{1}{3}\left(2^{2l-1} + (-1)^l.2^{l-1} - 1\right).$$

Therefore R_β in the even case depends on β. Let β be such an element that $\gamma = \beta^{2^s} + \beta$ is a cube. Then $(\beta^{2^s} + \beta)/t^{2^s+1}$ takes any nonzero cubes 3 times when t runs through $GF(2^m)^*$. According to Lemma 2 the number of cubes with zero trace is p. Hence, for any fixed β, i.e. the pair $\{0, j\}$, such that $\gamma = \beta^{2^s} + \beta$ is a cube, we have

$$R_\beta = 3p.$$

Therefore the number of codewords of weight 5 and nonzero positions 0 and j corresponding to such a β is

$$\lambda = p - 1 = \frac{1}{3}\left(2^{2l-1} - (-1)^l.2^l - 4\right).$$

Similarly, let β be such an element that $\gamma = \beta^{2^s} + \beta$ is of the type α^{3k+1} (respectively α^{3k+2}). Then $(\beta^{2^s} + \beta)/t^{2^s+1}$ takes any nonzero elements of the type α^{3k+1} (respectively α^{3k+2}) 3 times when t runs through $GF(2^m)^*$. But exactly q of them have zero trace and hence for so chosen β we have $R_\beta = 3q$. Therefore the number of codewords with weight 5 and nonzero positions 0 and j corresponding to so chosen β is

$$\mu = q - 1 = \frac{1}{3}\left(2^{2l-1} + (-1)^l.2^{l-1} - 4\right).$$

To complete the proof we should calculate the number of β (i.e. the number of j) for which $\gamma = \beta^{2^s} + \beta$ is a cube and the one for which γ is of the type α^{3k+1}, respectively α^{3k+2}. Since $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\beta) + \mathrm{Tr}(\beta) = 0$ the number of cubes is given again by Lemma 2. But γ is obtained for exactly two values of β according to Lemma 3. Thus γ is a cube for $2p$ values of β, i.e. for $2p$ values of j.

Similarly, for $2q$ values of β, γ is of the type α^{3k+1} and for $2q$ values is of the type α^{3k+2}.

Therefore, for

• $2p$ pairs $\{0, j\}$ the number of codewords of weight 5 with nonzero 0^{th} and j^{th} positions is

$$\lambda = p - 1 = \frac{1}{3}\left(2^{2l-1} - (-1)^l.2^l - 4\right).$$

• $4q$ pairs $\{0, j\}$ the number of codewords of weight 5 with nonzero 0^{th} and j^{th} positions is

$$\mu = q - 1 = \frac{1}{3}\left(2^{2l-1} + (-1)^l.2^{l-1} - 4\right).$$

Since any pair $\{i, j\}$ will be counted two times as a pair $\{0, h\}$ we get
• for $np = n.2p/2$ pairs $\{i, j\}$

$$\lambda = p - 1 = \frac{1}{3}\left(2^{2l-1} - (-1)^l.2^l - 4\right).$$

• for $2nq = n.4q/2$ pairs $\{i, j\}$

$$\mu = q - 1 = \frac{1}{3}\left(2^{2l-1} + (-1)^l.2^{l-1} - 4\right). \qquad \square$$

Since in any codeword of weight 5 there are $\binom{5}{2} = 10$ pairs of nonzero coordinates, then

$$10A_5 = \binom{n}{2}\lambda, \quad \text{respectively,} \quad 10A_5 = np.\lambda + 2nq.\mu$$

which yields, in particular, the value (well known, [16, Ch.15]) of A_5 :

$$A_5 = \begin{cases} \dfrac{n(n-1)(n-7)}{120}, & m = 2l+1 \\ \dfrac{n(n-3)^2}{120}, & m = 2l. \end{cases}$$

Note: Lemma 4 gives that when m is odd the number of codewords of weight 3 in any coset of $\mathcal{C}$ with a leader of weight 2 is constant λ, i.e. the code $\mathcal{C}$ is "uniformly packed" (proved by Dumer). In the case of BCH codes ($s = 1$), λ was calculated by J. Goethals and H. van Tilborg [12]

Theorem 1. *Let $\mathcal{C}$ be a binary cyclic code of length $n = 2^m - 1$ and a generator polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, where $(s, m) = 1$.*

If $m = 2l + 1$, then the number of minimal codewords of weight 10 *is*

$$M_{10} = A_{10} - \frac{n(n-1)(n-7)(n-17)(n^2-16n+135)}{2.120^2}.$$

If $m = 2l$, then the number of minimal codewords of weight 10 *is*

$$M_{10} = A_{10} - \frac{n}{144}\left[\frac{(n-5)(n^4 - 32n^3 + 394n^2 - 2008n + 4861)}{200} - (-1)^l 2^{3l+1}\right].$$

Theorem 2. *Let $\widehat{\mathcal{C}}$ be the extended $[2^m,\ 2^m - 2m - 1,\ 6]$ code of the binary cyclic code of length $n = 2^m - 1$ and a generator polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, where $(s, m) = 1$.*

In the case $m = 2l + 1$, the number of minimal codewords of weight 12 *equals*

$$\widehat{M}_{12} = \widehat{A}_{12} - \frac{\lambda}{4}\binom{n+1}{3}\left[\lambda\frac{(n^2 - 35n + 450)(n-1)}{1200} - 1 - \frac{1}{3}(\lambda - 1)(\lambda + 4)\right],$$

where $\lambda = (n - 7)/6$.

In the case $m = 2l$,

$$\widehat{M}_{12} = \widehat{A}_{12} - \frac{n(n+1)}{6}\left\{\frac{(n-3)^2}{240}\left[\frac{(n^2 - 35n + 450)(n-3)^2}{720} - 10\right]\right.$$
$$\left. - \left[(\lambda + 4)\binom{\lambda+1}{3} + 2(\mu + 4)\binom{\mu+1}{3}\right]\right\},$$

where λ, μ are given by Lemma 4, *$\widehat{A}_{12}$ is the number of codewords of weight* 12.

The values λ and μ given in Lemma 4 do not depend on the value of s and coincide with the ones for $s = 1$. Hence, not only the statements of Theorem 1 and Theorem 2 but also their proofs are very similar to the case of BCH codes. Also, there are several common and similar steps in the proofs of both theorems. That is why, herein we omit detailed calculations (referring the reader to our paper [6]) and present only the idea and the main points of these proofs.

Proof of Theorem 1 and Theorem 2. Since the minimum distance of $\mathcal{C}$ (resp. $\widehat{\mathcal{C}}$) is 5 (resp. 6), a codeword of weight 10 (resp. 12) is non-minimal **iff** it is a sum of two nonintersecting codewords of weight 5 (resp. 6). Since two codewords of weight 5 can intersect each other in 2 coordinates at the most, any non-minimal codeword of weight 10 can be uniquely split into a sum of two codewords $c_1, c_2 \in \mathcal{C}$ of weight 5. Thus the number of non-minimal codewords of weight 10 in $\mathcal{C}$ coincides with the number N_0 of pairs of codewords

of weight 5 with disjoint supports. (Respectively, $\widehat{N}_0$ denotes the number of pairs of codewords of weight 6 in $\widehat{\mathcal{C}}$ with disjoint supports.) But in the case of the extended code the expression of $\widehat{\mathbf{c}} \in \widehat{\mathcal{C}}$ of weight 12 as a sum of two codewords of weight 6 is not always unique, which makes the proof of Theorem 2 more complicated. In this case the number of non-minimal codewords of weight 12 is $\widehat{N}_0 - 2Y$, where Y is the number of codewords $\widehat{\mathbf{c}} \in \widehat{\mathcal{C}}$ of weight 12 that admit more than one (exactly three) expression as a sum of two words of weight 6. Indeed since the supports of two codewords of $\widehat{\mathcal{C}}$ intersect each other in three elements at the most, then $\widehat{\mathbf{c}} = \mathbf{u}_1 + \mathbf{u}_2 = \mathbf{v}_1 + \mathbf{v}_2$ gives $wt(\mathbf{u}_i * \mathbf{v}_j) = 3$. Hence the 12 nonzero positions of $\widehat{\mathbf{c}}$ are divided into four triples, each two of which form a codeword of weight 6, and $\widehat{\mathbf{c}}$ has exactly three representations as a sum of words of weight 6. If X is the number of non-minimal codewords of weight 12, then $X + 3Y = \widehat{N}_0$. Therefore, the number of non-minimal codewords of weight 12 is equal to $X + Y = \widehat{N}_0 - 2Y$.

In both proofs we use the inclusion-exclusion principle. Let N_i (resp. $\widehat{N}_i$) be the number of pairs $\{c_1, c_2\}$ of weight 5 (resp. 6) with $wt(c_1 * c_2) \geq i$, i. e. the codewords have 1's at least on i common positions. Then

$$N_0 = N - N_1 + N_2 - N_3 + N_4 - N_5 + N_6, \tag{5}$$

where $N = \binom{A_5}{2}$ $\left(\text{resp. } \widehat{N} = \binom{\widehat{A}_6}{2}\right)$ is the number of pairs of codewords. Let us note that $N_i = 0$, for $i \geq 3$, respectively for $i \geq 4$ in Theorem 2.

The automorphism groups of both considered codes are transitive: $\mathcal{C}$ is cyclic, and $\widehat{\mathcal{C}}$ is invariant under the affine group of permutations (Kasami et al. [14]). Therefore:

– We may assume w.l.o.g. that one of the common nonzero coordinate position is ∞. Thus

$$\widehat{N}_1 = 2^m N, \qquad \widehat{N}_2 = \frac{2^m}{2} N_1 \qquad \widehat{N}_3 = \frac{2^m}{3} N_2.$$

– The number r of $\mathbf{c} \in \mathcal{C}$ of weight 5 with common nonzero i^{th} coordinate is one and the same for any i and obviously $r = 5A_5/n$. Hence

$$N_1 = n\binom{r}{2}, \qquad n = 2^m - 1.$$

According to Lemma 4 the value N_2 depends on the parity of m, namely,

– if $m = 2l + 1$, then

$$N_2 = \binom{n}{2}\binom{\lambda}{2},$$

where $\lambda = (n-7)/6$ is determined in Lemma 4;

– if $m = 2l$, then

$$N_2 = n\left[p\binom{\lambda}{2} + 2q\binom{\mu}{2}\right],$$

where λ and μ are given in Lemma 4.

Now replacing values of N_i and $\widehat{N}_i$ in (5) and in the corresponding formula for $\widehat{\mathcal{C}}$, after simple computations we obtain N_0 (hence, M_{10}) and $\widehat{N}_0$.

Let us calculate Y.

$$Y = \frac{2^m}{3}\frac{1}{4}Z,$$

where Z is the number of triples of codewords of weight 6 with nonzero coordinates $\{i, j, \infty\}$. Then applying again Lemma 4 we get

– if $m = 2l + 1$, then

$$Y = \frac{n+1}{12}\binom{n}{2}\binom{\lambda}{3}, \qquad \lambda = \frac{n-7}{6};$$

– if $m = 2l$, then

$$Y = \frac{n+1}{12}\left[np\binom{\lambda}{3} + 2nq\binom{\mu}{3}\right].$$

Now we can calculate $\widehat{N}_0 - 2Y$ which gives the statement of Theorem 2. □

As a consequence of Lemma 1 and Theorem 2 we obtain

Theorem 3. *The number of minimal codewords of weight* 11 *in the double-error correcting* $[2^m - 1,\ 2^m - 2m - 1,\ 5]$ *binary code* $\mathcal{C}$ *with generator polynomial* $g(x) = m_1(x)m_{2^s+1}(x)$, *where* $(s, m) = 1$, *is*

$$M_{11} = \frac{3}{2^{m-2}}.\widehat{M}_{12},$$

where $\widehat{M}_{12}$ *is the number of minimal codewords of weight* 12 *in the extended code* $\widehat{\mathcal{C}}$.

4. Minimal codewords in the 3rd order binary Reed-Muller codes. A well-known and widely used approach to studying algebraic objects (groups, rings, etc.) is the considering of their sub-objects and quotient objects. Since linear codes are linear spaces this approach is applicable to them and it is often used in algebraic coding theory.

Let $\mathcal{C}$ be a linear code over the finite field $\mathbb{F} = GF(q)$ and G be a group of its automorphisms. If $\mathcal{A}$ is a $G-$invariant subcode (i.e. $\varphi(\mathcal{A}) \subseteq \mathcal{A}$ for any $\varphi \in G$) then G naturally induces an action on the quotient space $\mathcal{C}/\mathcal{A}$ consisting of all cosets $c+\mathcal{A}$, $c \in \mathcal{C}$. If $\varphi \in G$ preserves a given property and $\varphi : c_1+\mathcal{A} \longrightarrow c_2+\mathcal{A}$, then both $c_1+\mathcal{A}$ and $c_2+\mathcal{A}$ possess (or do not possess) this property. Therefore, knowing the partition of $\mathcal{C}/\mathcal{A}$ into $G-$orbits, one can restrict oneself only to the representatives of the orbits when studying the codewords with this property.

The described idea has been applied to solving weight distribution problems in [8] and [19] as well as by Hou (see [13]). Our study is based on the following results from the aforesaid papers:

Let $Q(r,m) \stackrel{\text{def}}{=} RM(r,m)/RM(r-1,m)$ be the quotient space of $RM(r,m)$ by the subcode $RM(r-1,m)$. On $Q(r,m)$ the action of $GA(m,2)$ is reduced to the action of the general linear group $GL(m,2)$, since the transformation $\mathbf{x} \to \mathbf{x}+\mathbf{a}$ leaves every element of $Q(r,m)$ fixed for any $\mathbf{a} \in GF(2)^m$.

Xiang-dong Hou has calculated the number of $GL(m,2)-$orbits and has determined explicitly the representatives of the cosets $h + RM(2,m)$ for $r = 3$ and $m \leq 8$.

Theorem 4 ([13]). *Let $s(r,m)$ denote the number of $GL(m,2)-$orbits in $Q(r,m)$. Then*

a) $s(3,6) = 6$ *and* $\mathcal{C}_i = f_i + RM(2,6)$, $1 \leq i \leq 6$, *are representatives of the $GL(m,2)-$orbits in $Q(3,6)$,*

b) $s(3,7) = 12$ *and* $\mathcal{C}_j = f_j + RM(2,7)$, $1 \leq j \leq 12$, *are representatives of the $GL(7,2)-$orbits in $Q(3,7)$,*

where the Boolean polynomials $f_i(\mathbf{x})$ are given by

$$\begin{aligned} f_1 &= 0, \\ f_2 &= x_1x_2x_3, \\ f_3 &= x_1x_2x_3 + x_2x_4x_5, \\ f_4 &= x_1x_2x_3 + x_4x_5x_6, \end{aligned}$$

$$
\begin{aligned}
f_5 &= x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6,\\
f_6 &= x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6,\\
f_7 &= x_1x_2x_7 + x_3x_4x_7 + x_5x_6x_7,\\
f_8 &= x_1x_2x_3 + x_4x_5x_6 + x_1x_4x_7,\\
f_9 &= x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_4x_7,\\
f_{10} &= x_1x_2x_3 + x_4x_5x_6 + x_1x_4x_7 + x_2x_5x_7,\\
f_{11} &= x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6 + x_1x_6x_7,\\
f_{12} &= x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6 + x_1x_6x_7 + x_2x_4x_7.
\end{aligned}
$$

Remark. Note that $\mathcal{C}_i = f_i + RM(2,m)$, $1 \le i \le 6$, are representatives of the $GL(m,2)-$orbits for $m \ge 6$, $\mathcal{C}_i$, $7 \le i \le 12$, for $m \ge 7$, and so on.

Following the notations in [19], for a given $f \in \mathcal{P}_m$, let $m(f)$ denote the minimal integer n for which there is such a transformation $T \in GL(m,2)$ and a polynomial $g \in \mathcal{P}_n$ that $T(f) \equiv g \,(\mathrm{mod}\, RM(r-1,m))$. For $f \in RM(r,m)$, let $\nu(r,m,f)$ denote the *number of cosets in the* $GL(m,2)-$*orbit of* $f+RM(r-1,m)$. Theorem 5 gives a recursion for $\nu(r,m,f)$.

Theorem 5 ([19])**.**

$$\nu(r,m,f) = \nu(r,m(f),f) \prod_{i=0}^{m(f)-1} (2^{m-i}-1)/(2^{m(f)-i}-1).$$

For $f \in \mathcal{P}_m$, $\deg f = 3$ and $\mathbf{a} \in GF(2)^m$ let $f_{\mathbf{a}}$ be the Boolean polynomial obtained from $f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x})$ by deleting all linear terms. Obviously, $f_{\mathbf{a}}$ is a homogenous polynomial of degree 2. The next theorem is Lemma 2 from [8] slightly modified for our goals.

Theorem 6 ([8])**.**

(a) $\Delta f = \{f_{\mathbf{a}} \mid \mathbf{a} \in GF(2)^m\}$ *is a linear subcode of* $RM(2,m)$.

(b) *Let the subspace* δf *of* $RM(2,m)$ *be defined by* $RM(2,m) = \Delta f \oplus \delta f$ *(direct sum).* δf *is invariant under the transformation* $\mathbf{x} \to \mathbf{x}+\mathbf{a}$ *for any* $\mathbf{a} \in GF(2)^m$.

(c) *The weight enumerator of minimal codewords of the coset* $f + RM(2,m)$ *is given by* $2^{\dim \Delta f} W_{f+\delta f}(z)$, *where* $W_{f+\delta f}(z)$ *is the weight enumerator of minimal codewords of the coset* $f + \delta f$.

Herein we determine the weight distribution of minimal codewords in Reed-Muller codes $RM(3,6)$ and $RM(3,7)$. These codes have parameters $[64,42,8]$ and $[128,64,16]$, respectively. It is obvious that a search for minimal codewords based on (iv) of Proposition requires too much computer resource even for such small parameters. Therefore we will apply the method described above.

Let M_w and $M_w^{(i)}$ denote the *number of minimal codewords of weight* w *in* $RM(3,m)$ *and in the coset* $\mathcal{C}_i$, respectively. Hence

$$M_w = \sum_i \nu(3,m,f_i) M_w^{(i)}. \tag{6}$$

Below we will refer several times to the following simple property of Boolean polynomials. Its proof is straightforward and we omit it.

Lemma 5. *Let* $f \in \mathcal{P}_m$ *be such that* $(x_i + a)f(\mathbf{x}) \equiv 0$ *for a given variable* x_i*, where* $a = 0$ *or* 1*. Then either* $f(\mathbf{x}) \equiv 0$*, or* $f = (x_i + a + 1)h(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m)$*, where* h *is a polynomial of* $m-1$ *variables and* $\deg h = \deg f - 1$.

Theorem 7. *The numbers of minimal codewords of weight* w *in* $\mathcal{C}_i$ *for* $i = 1, 2, 3, 7$ *are*

$$M_w^{(1)} = 0; \quad M_w^{(2)} = \begin{cases} 8 & , w = 2^{m-3} \\ 0 & , otherwise. \end{cases}; \quad \sum_w M_w^{(3)} \le 2^{m+1} \quad \sum_w M_w^{(7)} \le 2^{m+1}.$$

P r o o f. Let $S(f) = \mathrm{supp}(\mathbf{f})$ denote the support of the binary vector $\mathbf{f}$ associated with a Boolean polynomial $f(\mathbf{x})$.

When $f \in \mathcal{C}_1$, i.e. $f \in RM(2,m)$, we have $x_i f \in RM(3,m)$ and $S(x_i f) \subseteq S(f)$ for any i. If $\mathbf{f}$ remains minimal as a codeword of $RM(3,m)$ then $x_i f(\mathbf{x}) \equiv 0$ or $x_i f(\mathbf{x}) \equiv f(\mathbf{x})$, i.e. $(x_i + 1)f(\mathbf{x}) \equiv 0$. (Note that a codeword of $RM(2,m)$ can be minimal in $RM(2,m)$ but non-minimal as a codeword of $RM(3,m)$.) Now applying Lemma 5, we conclude that $f(\mathbf{x}) = (x_1+a_1)(x_2+a_2)(x_3+a_3)f'(x_4, \ldots, x_m)$ for some $a_i = 0$ or 1. That is in contradiction to the choice of f. Therefore, $\mathcal{C}_1$ does not contain minimal codewords of $RM(3,m)$.

Let $f \in \mathcal{C}_2$, i.e. $f(\mathbf{x}) = x_1x_2x_3 + g(\mathbf{x})$, where $g \in RM(2,m)$. In this case $x_i f \in RM(3,m)$ only for $i = 1,2,3$. Similarly to the previous case we can conclude that the assumption $\mathbf{f}$ is minimal in $RM(3,m)$ implies $f(\mathbf{x}) = (x_1 + a_1)(x_2 + a_2)(x_3 + a_3)$, $a_i = 0, 1$. The eight codewords $\mathbf{f}$ corresponding to these polynomials have weight 2^{m-3}. But this is the minimum weight of

$RM(3,m)$ and, thus, they are minimal codewords. Therefore, there are exactly 8 minimal codewords all of weight 2^{m-3} which belong to the coset $\mathcal{C}_2$.

Let $f \in \mathcal{C}_3$, i.e. $f(\mathbf{x}) = x_2(x_1x_3+x_4x_5)+g(\mathbf{x})$, where $g \in RM(2,m)$. Then $x_2f = x_2(x_1x_3+x_4x_5)+x_2g(\mathbf{x})$ belongs to $RM(3,m)$ and the assumption that $\mathbf{f}$ is a minimal codeword of $RM(3,m)$ again implies $x_2f(\mathbf{x}) \equiv 0$ or $(x_2+1)f(\mathbf{x}) \equiv 0$. But $x_2f(\mathbf{x}) = x_2(x_1x_3 + x_4x_5 + g(\mathbf{x}))$. Hence, $x_2(x_1x_3 + x_4x_5 + g(\mathbf{x})) \equiv 0$ and Lemma 5 give $g(\mathbf{x}) = x_1x_3 + x_4x_5 + (x_2+1)g'(x_1,x_3,\ldots,x_m)$, where g' is a linear Boolean polynomial. Therefore there are only 2^m such polynomials $f(\mathbf{x})$. The second case implies $(x_2+1)g(\mathbf{x})) \equiv 0$ and Lemma 5 gives $g(\mathbf{x}) = x_2g'(x_1,x_3,\ldots,x_m)$, where g' is a linear Boolean polynomial. Therefore, the total number of minimal codewords in $\mathcal{C}_3$ is at most $2 \cdot 2^m = 2^{m+1}$. ($|\mathcal{C}_i| = |RM(2,m)| = 2^{1+m+\binom{m}{2}}$!)

The case $\mathcal{C}_7$ is treated in the similar way and the same result holds for it. □

Theorem 8. *The distribution of minimal codewords of weight w in $RM(3,6)$ is given in Table 2.*

P r o o f. For $RM(3,6)$ the possible weights for which both minimal and non-minimal codewords can exist are 16,18,20 and 22. Since there are no codewords of weight 10 in $RM(3,6)$ then all codewords of weight 18 are minimal. Based on the above-mentioned, we have to test for minimality only the codewords in $\mathcal{C}_4$, $\mathcal{C}_5$, $\mathcal{C}_6$ and 128 codewords in $\mathcal{C}_3$. For f_i, $i = 4,5,6$, we determine Δf_i and δf_i. According to Theorem 4 our search is restricted only to $f_i + \delta f_i$. This reduces computational complexity by a factor $2^{\dim \Delta f_i}$. In our case based on the definition, it is not difficult to check that $\dim \Delta f_i = 6$, $i = 4,5,6$, and to find a basis of δf_i. Then we determine the values of $M_w^{(i)}$, $i = 3,4,5,6$, by computer search.

i	$\nu(3,6,f_i)$	i	$\nu(3,7,f_i)$	i	$\nu(3,7,f_i)$
1	1	1	1	7	1 763 776
2	1 395	2	11 811	8	2 222 357 760
3	54 684	3	2 314 956	9	238 109 760
4	357 120	4	45 354 240	10	17 778 862 080
5	468 720	5	59 527 440	11	444 471 552
6	166 656	6	21 165 312	12	13 545 799 680

Table 1. Lengths of the orbits with representatives $\mathcal{C}_i$ in $RM(3,6)$ and $RM(3,7)$.

Knowing $M_w^{(i)}$ we can obtain the weight distribution of minimal codewords in $RM(3,6)$ by (6). The required values $\nu(3,6,f_i)$ have been determined by Hou [13]. Using $\nu(3,6,f_i)$, Theorem 4 and $\nu(3,8,f_i)$ given in [19, Table 1] the values of $\nu(3,7,f_i)$ can be calculated, too. All values are given in Table 1. The results for $M_w^{(i)}$ are summarized in Table 2. The symbol "$*$" means that all codewords of this weight are minimal. □

w	M_w
*8	11 160
*12	1 749 888
*14	22 855 680
16	213 486 336
*18	1 717 223 424
20	6 719 569 920
22	14 581 066 112

Table 2. The weight distribution of minimal codewords in $RM(3,6)$.

Theorem 9. *The distribution of minimal codewords of weight w in $RM(3,7)$ is given in Table 3.*

$RM(3,7)$ is treated in a similar manner. Interesting weights are 32, 36, 40, 44, 48, 52, 56, 60 and 64. Since there are no codewords of weight 20 in $RM(3,7)$ then all of weight 36 are minimal. In $\mathcal{C}_3$ and $\mathcal{C}_7$ only 256 codewords have to be tested (see the aforesaid). For any of the rest eight cosets we determine Δf_i and δf_i and restrict the computer search only to $f_i+\delta f_i$, where $\dim \Delta f_i = 6, i = 4,5,6$, and $\dim \Delta f_i = 7$ for $i \geq 8$. The obtained results are given in Table 3. □

w	M_w	w	M_w
*16	94 488	44	9 482 818 340 782 080
*24	74 078 592	48	87 824 734 057 267 200
*28	3 128 434 688	52	538 097 941 223 571 456
32	311 574 557 952	56	1 752 914 038 641 131 520
*36	18 125 860 315 136	60	2 787 780 190 808 309 760
40	551 965 599 940 608	64	517 329 044 342 046 720

Table 3. The weight distribution of minimal codewords in $RM(3,7)$.

In conclusion we would like to note that during the process of computer searching we obtain the representative of the orbits of minimal codewords. Hence,

nevertheless, only the number of minimal codewords is given herein, we can list all minimal codewords.

Acknowledgements. This research was partially supported by the Bulgarian NSF under Contract I-1301/2003.

REFERENCES

[1] E. Agrell. Voronoi Regions for Binary Linear Codes. *IEEE Trans. Inf. Theory* **IT-42**, *1* (1996), 310–316.

[2] A.A shikhmin, A. Barg. Minimal Vectors in Linear Codes. *IEEE Trans. Inf. Theory* **IT-44**, *5* (1998), 2010–2017.

[3] A. Barg. Complexity issues in coding theory in Handbook of Coding Theory. (Eds V. Pless and W. Huffman) Amsterdam, Elsevier Science B.V., 1998.

[4] T. Berger. Automorphism Groups and Permutation Groups of Affine-Invariant Codes. In: Finite Fields and Applications. Proceedings of the 3rd International Conference (Eds S. Cohen et al.) Glasgow, UK, July 11-14, 1995, Cambridge: Cambridge University Press, Lond. Math. Soc. Lect. Note Ser., vol. **233** (1996), 31–45.

[5] E. Berlekamp. Algebraic Coding Theory. McGraw-Hill, New York, 1968.

[6] Y. Borissov, N. L. Manev. Minimal words of the primitive BCH codes. *Problems of Information Transmission* **34**, *3* (1998), 238–246.

[7] Y. Borissov, N. Manev, S. Nikova. On the non-minimal codewords in binary Reed-Muller codes. *Discrete Appl. Math.* **128** (2003), 65–74.

[8] Y. Desaki, T. Fujiwara, T. Kasami. The weight distribution of extended binary primitive BCH codes of length 128. *IEEE Trans. Inf. Theory* **IT-43**, *4* (1997), 1364–1371.

[9] S. M. Dodunekov. Some Quasi-perfect Double Error Correcting Codes. *Problems Control Inform. Theory* **15**, *5* (1986), 367–375.

[10] I. Dumer. Some new uniformly packed codes. *Trudy MFTI* (1976), 72-78 (in Russian).

[11] Tai-Yang Hwang. Decoding linear block codes for minimizing word error rate. *IEEE Trans. Inform. Theory* **IT-25**, *6* (1979), 733–737.

[12] J. Goethals, H. van Tilborg. Uniformly packed codes. *Philips Res. Reports* **30** (1975), 9–36.

[13] X. Hou. $GL(m,2)$ acting on $R(r,m)/R(r-1,m)$. *Discrete Math.* **149** (1996), 99–122.

[14] T. Kasami, S. Lin, W. Peterson. Some results on cyclic codes which are invariant under the affine group and their application. *Inform. and Control* **11** (1968), 475–496.

[15] R. J. McEliece. Finite fields for computer scientists and engineers. The Kluwer International Series in Engineering and Computer Science – Information Theory, Kluwer Academic Publishers, Boston, 1987.

[16] F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes. North Holland, Amsterdam, 1977.

[17] J. Massey. Minimal Codewords and Secret Sharing. In: Proc. Sixth Joint Swedish-Russian Workshop on Inf. Theory. Molle, Sweden, 1993, 246–249.

[18] D. R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptography*, **2**, *4* (1992), 357–390.

[19] T. Sugita, T. Kasami, T. Fujiwara. The weight distribution of the third-order Reed-Muller code of length 512. *IEEE Trans. Inf. Theory* **IT-42**, *5* (1996), 1622–1625.

Appendix. Now we shall describe a way of constructing secret-sharing scheme by a binary linear code. Let $\mathcal{C}$ be a binary linear $[n,k]$-code, whose first coordinate is not always 0. Let the secret $\mathbf{s}$ be a binary vector with length l.

To any coordinate s_j of $\mathbf{s}$, $0 \leq j \leq l$, we add selected at random $k-1$ bits, which together with s_j (as a first coordinate) we use as set of information bits to compute the corresponding codeword of the code $\mathcal{C}$. Thus we obtain l codewords

and form by them an $l \times n$ matrix, the first column of which is the secret. The others are the $n-1$ shares in the secret-sharing scheme.

Obviously the access structure of this scheme is characterized by the set of minimal words with 1 as a first coordinate in the code $\mathcal{C}^{\perp}$.

Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria
e-mail: youri@moi.math.bas.bg
e-mail: nlmanev@moi.math.bas.bg

Received April 5, 2004